

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/565,663
Applicant(s) : Kamperman et al.
Filed : January 23, 2006
Conf. No. : 2420
TC/A.U. : 2456
Examiner : Richard G. Keehn
Atty. Docket : NL 030926
Title : Hybrid device and person based authorized domain architecture

REPLY BRIEF

Mail Stop **Appeal Brief – Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This Reply Brief is being submitted in response to the Examiner's Answer that was mailed on April 28, 2011 in connection with the above-identified patent application.

Claims 1, 3, 4, 6 – 12, 14, 15 and 17 – 23 stand rejected under 35 U.S.C. §103(a), over Nakahara et al. (US 2003/0018491), hereinafter Nakahara and further in view of Andrews et al. (US 6,324,645 B1), hereinafter Andrews.

Independent Claim 1

The subject matter, as recited in independent claim 1, relates to a method of generating an Authorized Domain (AD), the method comprising:

selecting a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (AD),
binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID),

binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID), and
binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) given by
the domain identifier (Domain_ID),
thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN₁) that are authorized to access content items (C1, C2, ..., CN₂) of said Authorized Domain (AD)
wherein access to the at least one content item (C1, C2, ..., CN₂) is obtained, via an
authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN₂) and the at
least one user (P1, P2, ..., PN₁) are linked to the same domain identifier (Domain_ID) or by verifying
that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN₂) are
linked to the same domain identifier (Domain_ID);
wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder
of the authorization certificate.

Independent Claim 12

The subject matter, as recited in independent claim 12, relates to a system for generating an
Authorized Domain (AD), the system comprising:
means for obtaining a domain identifier (Domain_ID) uniquely identifying the Authorized
Domain (AD),
**means for binding at least one user (P1, P2, ..., PN₁) to the domain identifier
(Domain_ID),**
means for binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID),
and
means for binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD)
given by the domain identifier (Domain_ID),
thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN₁) that is authorized to access content items (C1, C2, ..., CN₂) of said Authorized Domain (AD)
wherein access to the at least one content item (C1, C2, ..., CN₂) is obtained, via an
authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN₂) and the at
least one user (P1, P2, ..., PN₁) are linked to the same domain identifier (Domain_ID) or by verifying
that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN₂) are
linked to the same domain identifier (Domain_ID);
wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder
of the authorization certificate.

Appellant argues in the Appeal Brief, mail date February 15, 2011, that Nakahara does not teach or suggest at the Claim 1 step of:

binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID),

and Nakahara does not teach or suggest at the Claim 12 step of:

means for binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID),

Appellant argues that this step is not taught in Nakahara because the "Searcher X" cited in the reference is a pseudonym for a kind of role that a device unit may have, but not a user. (Brief at 15).

(A) In the Examiner's Answer, mail date April 28, 2011, the Examiner argues that the term "user" is not defined as a "person" or "human" in Claims 1 and 12. Therefore, using the broadest reasonable interpretation, a user may be a device. The Examiner further argues that there is nothing in claims 1 and 12 that make devices and users mutually exclusive.

Appellants assert that under long-standing precedent, the claims in a patent application pending at the U.S. Patent and Trademark Office ("PTO") are to be given their "broadest reasonable interpretation consistent with the specification." Moreover, "this interpretation must be consistent with the [interpretation] those skilled in the art would reach." Notwithstanding this explicit rule of construction, in some instances, such as the present case, examiners at the PTO have truncated the rule, applying the "broadest" construction, without regard to the specification or the perspective of the person skilled in the art. Such an interpretation may lead to an excessively broad reading of claim terminology and rejections

based upon references having little if anything to do with the claimed invention. Interpreting claims in this fashion is contrary not only to the rule of construction but also the PTO's own guidelines. **To avoid these problems, the rule must be properly and consistently applied.** In the present matter, Appellants assert that the Examiner has broadly construed a "user" to be a "device" without giving proper regard to the specification or the perspective of the person skilled in the art. Appellant's assert that the term "user" cannot be construed as a device in that the term "user" is used interchangeably with the term "person." The specification recites, "Accordingly, the present invention provides a method and corresponding system for providing an Authorized Domain structure based on both **persons** and devices." *See* published specification, par. 15. The specification further recites, "This invention relates to a system and a method of generating an Authorized Domain (AD) by selecting a domain identifier, and binding at least one **user** (P1, P, PN1), at least one device (D1, D2, . . . , DM), and at least one content item (C1, C2, . . . , CNZ) to the Authorized Domain (AD) given by the domain identifier (Domain ID). *See* published specification, Abstract.

(B) In the Examiner's Answer, mail date April 28, 2011, the Examiner further asserts that it is clear from par. 197 of Nakahara, which was cited in the Final Office Action, that person-binding is taught by the reference.

[0197] For example, even if **someone** connects an unauthorized terminal device located outside of the home network 300 to the home network 300 to acquire license information, **he** cannot acquire the license information because the terminal device **does not belong to the identical user domain**. Also, if different usage restrictions are put on a content usage device 1 for a **father's usage** and a content usage device 2 for his **son's usage** within the home network 300, these content usage devices can be classified so that the son cannot acquire the license information on the content usage device 2 though his father can acquire it on the content usage device 1.

Appellants assert that par. 197 does not show “person” binding. Instead, par. 197 clearly recites how “device” binding impacts various persons (e.g., someone, fathers, sons) associated with the device binding process. Appellants make similar disclosures in Appellant’s specification, referring to device binding in the context of an owner/user/person. For example, the specification recites, “If a user is visiting a friend’s house he is not able to access his legally purchased content on the friend’s devices as these devices would not typically be part of the particular and limited set of devices forming the domain comprising the user’s content.” *See* published specification, par. 10.

(C) **In the Examiner’s Answer, mail date April 28, 2011, the Examiner further asserts that Par. 198 of Nakahara clearly indicates authenticating the user domain. Taking this in context with pars. 14-16 and 197, where “a user can operate the content usage device”, it is clear that users can be people in Nakahara.**

Appellants respectfully assert that it is not clear that users can be people in Nakahara. In support, Appellants assert that par. 198 of Nakahara does not indicate “authenticating the user domain”. Nakahara at par. 198 clearly teaches in two places, “authenticating the function unit”, i.e., a device. Furthermore, taken in context of par. 14-16 of Nakahara, Appellants position is further supported in that **people** own and operate **devices**, as argued above and that Nakahara merely teaches that users can be devices.

[0198] Once receiving the request of the license information, the license management unit may **authenticate the function unit** that requests the license information according to SSL (Secure Sockets Layer) using a certificate pursuant to X.509 Protocol issued by CA (Certificate Authority), for instance, before it **authenticates using the user domain** and the usage restriction. In the above case, the license management unit that is requested the license information is only **authenticates the function unit** that requests it using the user domain and the usage restriction and the SSL. However, both the license management unit and the function unit may

authenticate each other.

(D) In the Examiner's Answer, mail date April 28, 2011, the Examiner further asserts that Appellant's also argue that that Nakahara does not disclose users as identifiers included in data structures, represented as elements of the domain structure. (Brief at 14).

The Examiner asserts that this is not claimed. The claims merely recite that users are merely bound to the domain as claimed, which does not make the user's "elements of the domain" as argued by Appellant. Independent claims 1 and 12 may be appropriately amended to recite this distinction. The Examiner asserts that Nakahara's father and son are certainly bound to the domain since their individual rights are being authenticated, which also makes the father and son identifiers in the domain.

Appellants respectfully disagree. Authenticating rights, by themselves, **do not bind persons entitled to those rights to a domain.** The invention discloses user rights (URC) which are analogous to the authenticating rights of Nakahara. **User rights do not make the users identifiers in the domain.** The specification clearly states that the devices, persons, and content items have been bound to the domain (100). Also shown are one or more user rights (URC1, . . . URCN.sub.2), where preferably one content item is associated with one user right certificate specifying which rights a given person (or alternatively a given group of persons and/or all persons bound to the domain (100)) have in relation to the specific content item (or alternatively, several or all content items in the domain (100)). It is therefore shown

that user rights (URC) do not bind persons entitled to those rights to a domain.

(E) In the Examiner's Answer, mail date April 28, 2011, the Examiner further asserts that Appellant's also argue that Nakahara does not teach or suggest the limitation binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) given by the domain identifier (Domain_ID), and thereby obtaining a number of devices (D1, D2, ..., DN) and a number of users (P1, P2,...PN) that are authorized to access content items (C1, C2,...CN₂) of said Authorized Domain (AD). (Brief at 15).

The Examiner asserts that, to support this assertion, Appellant argues that "content usage devices" are entirely different from "content items", but fails to argue or support how the broad claim term "item" has to be narrowly construed to exclude a device.

In response, Appellants assert that "content item" is a well-defined term which is never interpreted as a "content device". The common understanding of "content item" refers to a specific piece of content rather than "content" in general or a "content device". Appellant's specification clearly removes any ambiguity regarding how the term "content item" relates to "content" and never to a "content device". For example, the specification teaches "access to content", and "access to content item." Further, "license data" are not content items and cannot be fairly interpreted as such.

The Examiner relies once more on par. 197 of Nakahara and par. 193-194. Appellants re-assert that par. 197 does not show "person" binding. As argued supra, par. 197 clearly

recites how “device” binding impacts various persons (e.g., someone, fathers, sons) associated with the device binding process. Accordingly, the Examiner’s present argument fails in part for relying on par. 197. Irrespective of whether or not par. 193-194 teach licenses being bound to the domain, the Examiner has misconstrued the “broadest interpretation” guideline in suggesting that a broad interpretation of “item” is inclusive of “content usage devices”.

Appellant’s specification recites at par. 38, *In one embodiment, every content item is encrypted and that a content right is bound to each content item and to a User Right or a Device Rights or a Domain Rights, and that the content right of a given content item comprises an decryption key for decrypting the given content item.*”

Given the Examiner’s broadest reasonable interpretation, it follows that it is unreasonable to suggest that “content usage devices” are encrypted. Further, par. 92 of Appellant’s specification recites, *the content identifier (Cont_ID) for the given content item that the user wants to access and the person identifier (Pers_ID) of the user are obtained. The person identifier may e.g. be obtained on the basis of a personalized identification device (e.g. a smart card, mobile phone, a mobile phone containing a smartcard, a biometric sensor, etc. or in another way). The content identifier may e.g. be obtained on the basis of a file name, the selection of a file, from a header of the content container, etc.* It is clear that the specification clearly distinguishes “content usage devices”, as suggested by the Examiner by referring to content identifiers on the basis of criteria which has no nexus to “devices”, i.e., file names, selection of files, and headers.

(F) **In the Examiner's Answer, mail date April 28, 2011, the Examiner further asserts that Appellant's also argue that the cited references fail to disclose "inclusion of the domain id as a holder of the authorized certificate" by arguing that "According to the invention, a certificate creates or defines part of the domain." (Brief at 16).**

The Examiner asserts that he has to examine what is claimed and that the claim does not recite that "*a certificate creates or defines part of the domain*", as argued by Appellants. Instead, the claim limitation recites "*wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the authorization certificate.*"

The Examiner relied upon Andrews et al. to teach "includes the domain identifier (Domain_ID) as a holder of the authorized certificate" The Examiner asserts that clearly Andrews discloses this limitation at 9:49-58. This cited section teaches that the digital certificates contain an access label (holder) that is used to identify **which user(s)** have privileged access to content within a domain (holder of the certificate); and that access label includes a domain identifier. Even according to Appellant's argued definition of "a certificate creates or defines part of the domain", the domain identifier in Andrews identifies which domain the certificate applies to, which is "part of the domain". The Examiner states that, nonetheless, there is absolutely nothing in the language of the argued claims 1 and 12 that indicates that "a certificate creates or defines part of the domain". The Examiner further states that Appellant's argument that the claimed invention relates to content-access domains vs. Andrews relating to privilege / administrative domains is unpersuasive to the Examiner because both inventions relate to privileged access to content within a domain.

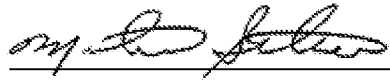
In response, Appellants assert that while both inventions may relate to privileged access to content within a domain, Appellant's respectfully submit that a certificate creates or defines part of the domain, while in Andrews, it refers to **members of the domain**. The types of domains referred to in Andrews is a **user** privilege/administrative domain, while the invention refers to **content-access domains**. The Examiner attempts to generalize both inventions by asserting that both inventions relate to privileged access to content within a domain, to find Appellant's argument unpersuasive. However, the generalization fails to capture essential differences between the two inventions, as argued above.

Further, in response to the Examiner's assertion that he can only examine what is claimed, Appellants assert that the claim limitation "*wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the authorization certificate*" can be reasonably construed as being equivalent to the unclaimed recitation of, "*a certificate creates or defines part of the domain.*" That is, by virtue of the certificate including the domain identifier (Domain_ID), the certificate inherently creates or defines part of the domain.

CONCLUSION

Appellants respectfully maintain that the rejections of claims are legally in error, legally and actually, and must be reversed.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Michael A. Scaturro", is written over a horizontal line.

Michael A. Scaturro
Reg. No. 51,356
Attorney for Appellants

Mailing Address:
Intellectual Property Counsel
Philips Electronics North America Corp.
P.O. Box 3001
345 Scarborough Road
Briarcliff Manor, New York 10510-8001